UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/577,625	04/28/2006	Audrius Berzanskis	053-03US1	5658

53590 7590 04/22/2008
OPTICUS IP LAW, PLLC
7791 ALISTER MACKENZIE DRIVE
SARASOTA, FL 34240

EXAMINER	
LAFORGIA, CHRISTIAN A	
ART UNIT	**PAPER NUMBER**
2139	
MAIL DATE	**DELIVERY MODE**
04/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/577,625	BERZANSKIS ET AL.	
	Examiner	**Art Unit**	
	Christian LaForgia	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _01 February 2008_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-13_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-13_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _28 April 2006_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. The amendment of 01 February 2008 has been noted and made of record.

2. Claims 1-13 have been presented for examination.

Response to Arguments

3. Applicant's arguments with respect to the prior art rejections of claims 1-13 have been considered but are moot in view of the new grounds of rejection.

4. See further rejections set forth below.

Specification

5. The amendment filed 01 February 2008 is objected to under 35 U.S.C. 132(a) because it introduces new matter into the disclosure. 35 U.S.C. 132(a) states that no amendment shall introduce new matter into the disclosure of the invention. The added material which is not supported by the original disclosure is as follows:

The amendment to the Specification to include "The collection of exchanged qubits is called the ‘raw key.’ Alice and Bob then use a public channel compare the bases used to measure the qubits and keep only those bits having the same basis. This collection of bits is called the ‘sifted key.’”

The amendment to independent claims 1, 8, and 9 to include “without first forming unencrypted qubits from the optical pulses.”

The amendment to independent claim 5 to include “simultaneously encoded and encrypt the optical pulses to form encrypted qubits.”

6. Applicant is required to cancel the new matter in the reply to this Office Action.

Claim Objections

7. Claims 10, 12, and 13 are objected to as being in improper form because claim 10 depends from itself. Claims 12 and 13 are objected to due to their dependency on claim 10. For the sake of examination, the Examiner will treat claim 10 as if it depends from claim 8.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

9. Claims 1-4 and 8-13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. The amendment of 01 February 2008 added the limitation "without having to first form unencrypted qubits" to independent claims 1, 8, and 9 (see similar but not necessarily identical claim language). After reviewing the specification for support for the amendment, the Examiner is unable to find any. MPEP § 2173.05(i) states that "the mere absence of a positive recitation is not basis for an exclusion." In other words, the fact that the specification provides for a method that does not explicitly state that unencrypted qubits are not formed prior to encryption is not enough support to provide for the exclusory limitation. The Applicant is required to show where support for the negative limitation is in the specification and, if they cannot, they are required to cancel said limitation.

10. Claims 5-7 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claims contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventors, at the time the application was filed, had possession of the claimed invention. The amendment of 01 February 2008 added the limitation “simultaneously encoded and encrypt the optical pulses to form encrypted qubits” to independent claim 5. After reviewing the specification for support for the amendment, the Examiner is unable to find any. The specification provides for a method that does not explicitly state simultaneously encoded and encrypt the optical pulses to form encrypted qubits and therefore does not provide enough support for the limitation. The Applicant is required to show where support for the limitation is in the specification and, if they cannot, they are required to cancel said limitation.

11. Claims 1-4 and 8-13 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claims contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Independent claims 1, 8 and 9 have been amended to include data that has not been previously disclosed in the specification or any of the originally presented claims. One of ordinary skill would not be replicate the method and systems of the claims in question, thereby requiring undue experimentation to make or use the invention. Since the making or using the invention would require undue experimentation, the claims fail to satisfy the requirements of 35 U.S.C. 112, 1st paragraph and are therefore rejected.

12. Claims 5-7 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claims contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Independent claim 5 has been amended to include data that has not been previously disclosed in the specification or any of the originally presented claims. One of ordinary skill would not be replicate the method and systems of the claims in question, thereby requiring undue experimentation to make or use the invention. Since the making or using the invention would require undue experimentation, the claims fail to satisfy the requirements of 35 U.S.C. 112, 1st paragraph and are therefore rejected.

Claim Rejections - 35 USC § 103

13. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

14. Claims 1 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,757,912 to Blow, hereinafter Blow, in view of U.S. Patent Application Publication No. 2004/0032954 A1 to Bonfrate et al., hereinafter Bonfrate.

15. As per claim 1, Blow teaches a method of performing quantum key distribution (QKD) (column 7, line 57), comprising a random set of bits that can be used to generate a key (column 10, lines 54-67).

16. Blow does not teach encrypting the key bits and using the encrypted key bits to form encrypted qubits.

17. Bonfrate discloses encoding key information and having single optical photons (qubits) carry said encoded key information (paragraph 0007).

18. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the encrypted the key bits to form encrypted qubits without first forming unencrypted qubits from the optical pulses, since Bonfrate states at paragraph 0007 that the quantum properties ensure that any attempt at eavesdropping during transit will yield only partial information on the key and will also generate errors that are detectable by the legitimate users, since any photon detected by an eavesdropper is likely either to fail to reach its intended destination or to have been changed by the detection process.

19. As per claim 9, Blow teaches a quantum cryptography system, comprising:

a) a quantum key distribution (QKD) that encodes weak optical pulses to form qubits (column 7, lines 57-67).

20. Blow does not teach key bits and basis bits and a classical encryption system operably coupled to the QKD system and adapted to encode at least one of the key bits and the basis bits to form encrypted qubits.

21. Bonfrate discloses encoding key information and having single optical photons (qubits) carry said encoded key information (paragraph 0007).

22. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the encrypted the key bits to form encrypted qubits without first forming unencrypted qubits from the optical pulses, since Bonfrate states at paragraph 0007 that the quantum properties ensure that any attempt at eavesdropping during transit will yield only partial information on the key and will also generate errors that are detectable by the legitimate users,

since any photon detected by an eavesdropper is likely either to fail to reach its intended destination or to have been changed by the detection process.

23. Claims 2-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Blow in view of Bonfrate as applied 1 above, and further in view of **Applied Cryptography**, to Bruce Schneier, hereinafter Schneier.

24. Regarding claim 2, Blow and Bonfrate do not teach encrypting the key bits using a stream cipher.

25. Schneier teaches the use of stream ciphers (pages 197-211).

26. One of ordinary skill in the art could have combined a stream cipher in the combined system of Blow and Bonfrate since Schneier discloses at page 197 that stream ciphers convert plaintext to ciphertext one bit at a time. This would have been the most practical solution since the Applicant is breaking the key into bits, Blow discloses a combination of secret bits used to formulate a key, and Bonfrate encrypts the data bit by bit to form quantum bits (aka qubits). See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

27. With regards to claim 3, Bonfrate teaches the use of a password (paragraphs 0044, 0045, 0072, 0076).

28. With regards to claim 4, Bonfrate teaches decoding the encrypted qubits on the receiving side (paragraph 0067). Schneier discloses the use of stream ciphers (pages 197-211).

29. As per claim 5, Blow teaches a method of performing quantum key distribution (QKD) (column 7, line 57) comprising a first QKD station that generates a random set of bits that can be used to generate a key (column 10, lines 54-67).

30. Schneier teaches generating a key stream using a key stream generator and then XORing that data to the plain text data to produce the stream of ciphertext bits (page 197).

31. One of ordinary skill in the art could have combined generate a pad (aka key stream) and XOR the pad with the key bits since Schneier discloses at page 197 that stream ciphers convert plaintext to ciphertext one bit at a time. This would have been the most practical solution since the Applicant is breaking the key into bits and Blow discloses a combination of secret bits used to formulate a key. See *KSR International Co. v. Teleflex Inc.*, 82 USPQ2d 1385 (U.S. 2007).

32. Blow and Schneier do not teach modulating weak optical pulses using the encrypted key bits to generate encrypted qubits.

33. The Applicant admits in the "Background Art" section of the specification that quantum key distribution involves establishing a key between a sender and receiver utilizing weak optical signals (page 2, Amendment to the Specification, 4/28/06). Since all of the references deal with quantum communications they all involved weak optical signals.

34. Bonfrate discloses encoding key information and having single optical photons (qubits) carry said encoded key information (paragraph 0007).

35. It would have been obvious to one of ordinary skill in the art at the time the invention was made to modulate the weak optical pulses using the encrypted key bits so as to simultaneously encoded and encrypt the optical pulses to form encrypted qubits, since Bonfrate states at paragraph 0007 that the quantum properties ensure that any attempt at eavesdropping

during transit will yield only partial information on the key and will also generate errors that are detectable by the legitimate users, since any photon detected by an eavesdropper is likely either to fail to reach its intended destination or to have been changed by the detection process.

36. Regarding claim 6, Bonfrate discloses "Quantum Cryptography: Public Key Distribution and Coin Tossing" to C.H. Bennett et al., hereinafter Bennett, at paragraph 0002. Bennett discloses that Bob (the receiver) decides randomly for each photon received whether to measure the photon rectilinear polarization or diagonal polarization (see Section III, page 3, first paragraph).

37. Bonfrate teaches decoding the encrypted qubits on the receiving side (paragraph 0067). Schneier discloses the use of stream ciphers, specifically XORs to encrypt/decrypt a stream (pages 197-211).

38. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Blow in view of Bonfrate as applied above, and in further view of U.S. Patent Application Publication No. 2002/0106084 A1 to Azuma et al., hereinafter Azuma.

39. With regards to claim 7, Blow and Bonfate do not teach establishing a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD station.

40. Azuma teaches establishing a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD

station (paragraph 0007, i.e. results obtained from the observation bases on the Alice and Bob sides that match are adopted as data).

41. It would have been obvious to one of ordinary skill in the art at the time the invention was made to establish a sifted key between the first and second QKD stations based on the key bits generated in the first QKD station and the key bits recovered in the second QKD station, since Azuma states at paragraph 0049 that establishing a sifted key prevents an eavesdropper from extracting the original data even if the quantum state was stolen.

42. Claims 8-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 5,675,648 to Townsend, hereinafter Townsend, in view of U.S. Patent Application Publication No. 2006/0120529 A1 to Gisin et al., hereinafter Gisin, and further in view of Schneier in view of Bonfrate.

43. As per claim 8, Townsend teaches a QKD system, comprising:

a) a first QKD station (Figure 4 [block 1]) having:

a. an optical radiation source adapted to emit weak optical pulses of radiation (Figure 4 [block 48], column 4, lines 34-48, column 6, lines 41-63);

d. a modulator arranged to receive the weak optical pulses and adapted to modulate the polarization or phase of the weak optical pulses based on the encrypted key bits to form encrypted qubits (Figure 4 [block 49], column 4, lines 34-55);

b) a second QKD station (Figure 4 [block 2]) optically coupled to the first QKD station (Figure 4 [block 3]) and having:

a. a second modulator adapted to receive and randomly polarization-modulate or phase-modulate the encrypted qubits (Figure 4 [block 52], column 4, lines 34-55, column 6, lines 41-63);

b. a detector for detecting the modulated encrypted qubits (Figure 2 [block 10], column 6, lines 1-40).

44. Townsend does not teach a first random number generator adapted to generate random numbers for use as first key bits.

45. Gisin teaches the use of a random number generator to prepare random quantum states (Figure 1 [blocks 14, 44], paragraph 0026, claim 7).

46. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a random number generator to generate random numbers for the key bits, since Schneier states at page 197 that a randomized key stream allows for perfect security since patterns and strings of similar numbers can result in the key being determined by an eavesdropper.

47. Townsend and Gisin do not teach a first e/d module coupled to the first random number generator to encrypt the key bits thereby forming encrypted key bits and a second e/d module coupled to the detector and adapted to recover from the modulated encrypted qubits second key bits corresponding to the first key bits.

48. Bonfrate discloses encoding key information and having single optical photons (qubits) carry said encoded key information (paragraph 0007).

49. It would have been obvious to one of ordinary skill in the art at the time the invention was made to use the encrypted the key bits to form encrypted qubits without first forming

unencrypted qubits from the optical pulses, since Bonfrate states at paragraph 0007 that the quantum properties ensure that any attempt at eavesdropping during transit will yield only partial information on the key and will also generate errors that are detectable by the legitimate users, since any photon detected by an eavesdropper is likely either to fail to reach its intended destination or to have been changed by the detection process.

50. Regarding claim 10, Schneier teaches wherein classical encryption system includes an encryption/decryption (e/d) module configured to perform XOR-ing of the key bits and a password to form encrypted key bits (page 197).

51. Regarding claim 11, Schneier teaches wherein the classical encryption system is adapted to generate the password using a stream cipher (page 197).

52. With regards to claim 12, Bonfrate teaches a phase modulator operably coupled to the classical encryption system and configured to impart a phase to each weak optical pulse based on one of said encrypted key bits (paragraphs 0008, 0012, 0015, 0028, 0031).

53. Concerning claim 13, Bonfrate teaches wherein the basis bits are encoded, and wherein the phase modulator is configured to encode each weak optical pulse with one of the encoded basis bits (paragraphs 0008, 0012, 0015, 0028, 0031).

Conclusion

54. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

55. The following patents are cited to further show the state of the art with respect to key distribution using quantum cryptography, such as:

United States Patent No. 6,529,601 B1 to Townsend, which is cited to show key distribution using quantum cryptography.

United States Patent No. 5,850,441 A to Townsend, which is cited to show key distribution using quantum cryptography.

United States Patent No. 7,298,848 B2 to Debuisschert, which is cited to show distributing a key using quantum cryptography.

United States Patent No. 5,764,765 A to Phoenix et al., which is cited to show key distribution using quantum cryptography.

56. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

57. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

58. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

59. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine L. Kincaid can be reached on (571) 272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

60. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

clf